인공지능 보안

-13-

랜섬웨어

랜섬웨어

- Ransomware = Ransom + Software
- 파일을 인질로 잡아 몸값을 요구하는 소프트웨어

랜섬웨어

- 공격자 입장에서 전세계 모든 인터넷 기기가 고객이 되어 지속적인 수익 창출 가능
- 가상화폐를 이용하여 추적이 불가능하고 공격 구조가 단순
- 몸값 지불시, 대부분 복구 ← 신뢰가 중요

랜섬웨어

- 기존 악성코드와의 차이
  - 정보를 유출하지 않음. 대신 정보를 암호화하여 접근하지 못하게 함.
  - 자기 자신을 숨기려고 하지 않음. 암호화 작업 후 금전적 대가 요구.
  - 악성코드 생성이 쉬움. 이미 공개되어 있는 강력한 암호화 알고리즘(RSA, AES 등)을 사용

랜섬웨어

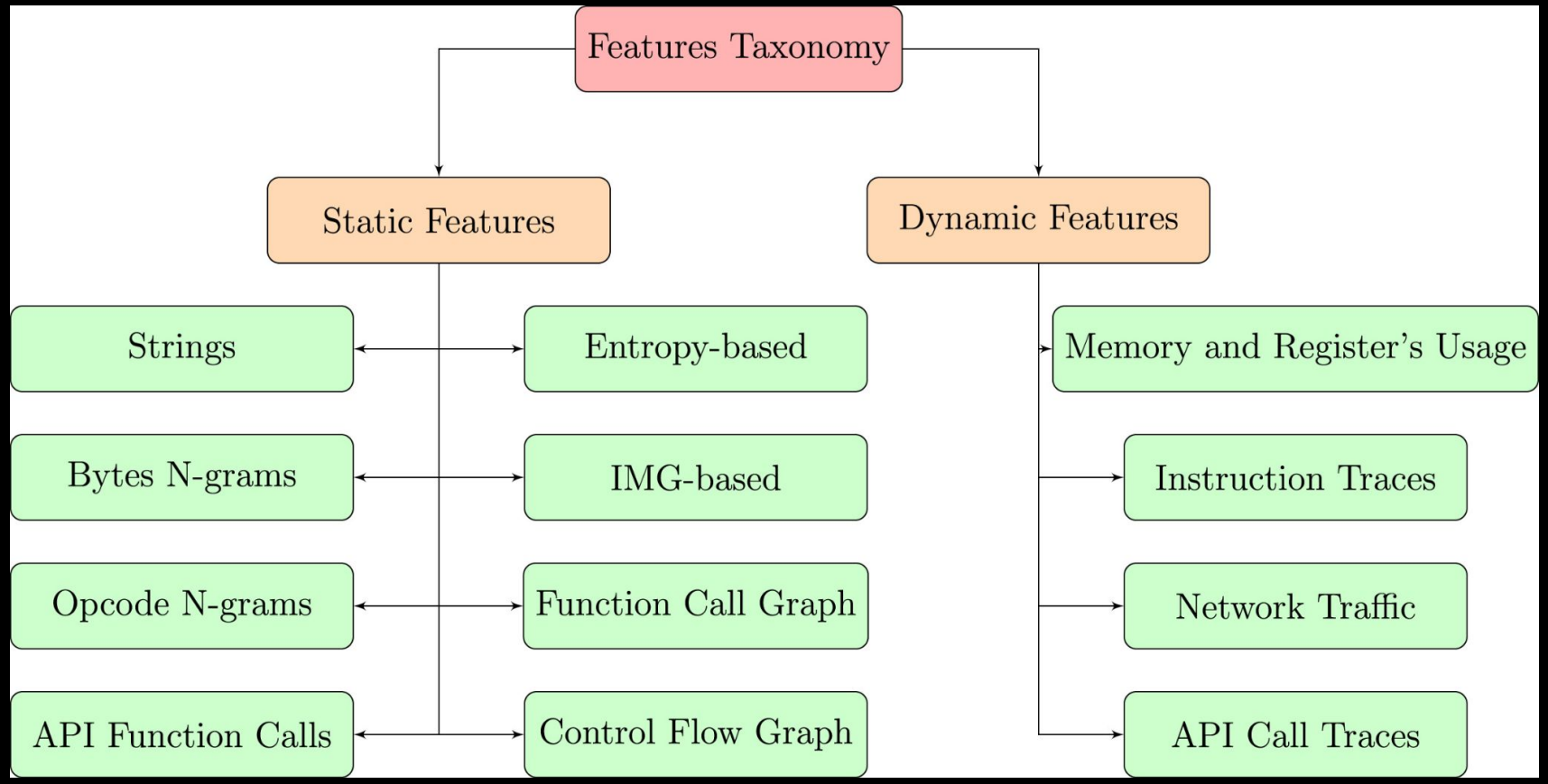
- 방어 / 대응 방법


랜섬웨어 공격 프로세스
1 포털 및 SNS 접속
2 악성코드 다운로드
3 랜섬웨어 동작
4 문서 파일 등 검색
5 암호화 수행
6 결제 유도
1 악성 및 의심스런 웹 사이트 접속 차단
2 네트워크 레벨 악성코드 분석 및 차단
3 의심 파일 실행 감지 및 차단
4 반복적인 파일 검색 등 의심 행위 감지 및 차단
5 다량의 파일 암호화 등 의심 행위 감지 및 차단
6 결제 유도 등 의심 행위 감지 및 차단
이상적인 랜섬웨어 '실시간 대응' 프로세스 (보안기술 활용 관점)

악성코드 탐지 with 인공지능

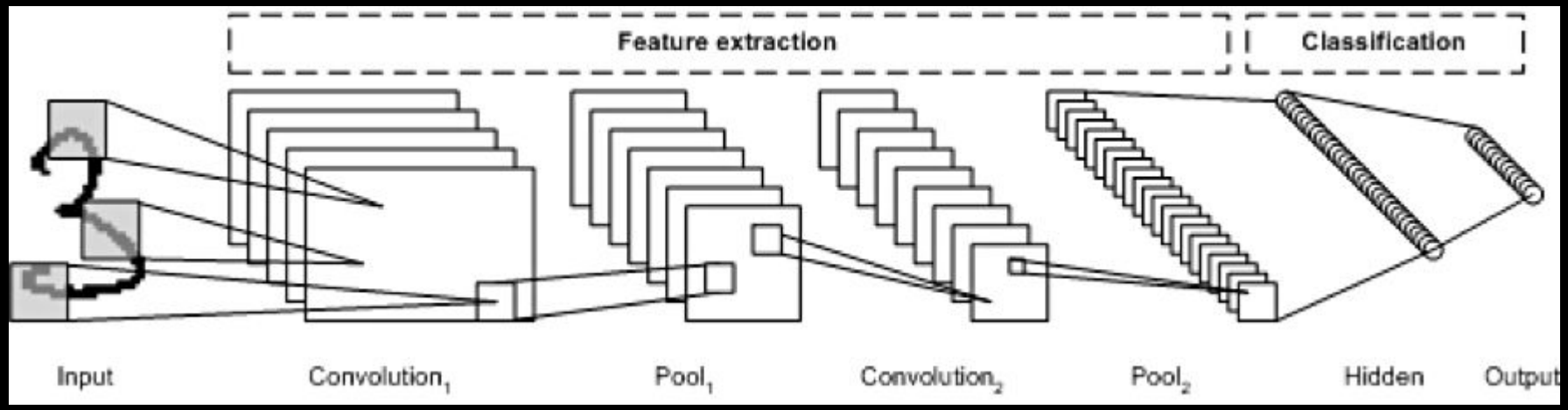
Malware Detection With M.L.

- Taxonomy of features used by M.L. approaches.



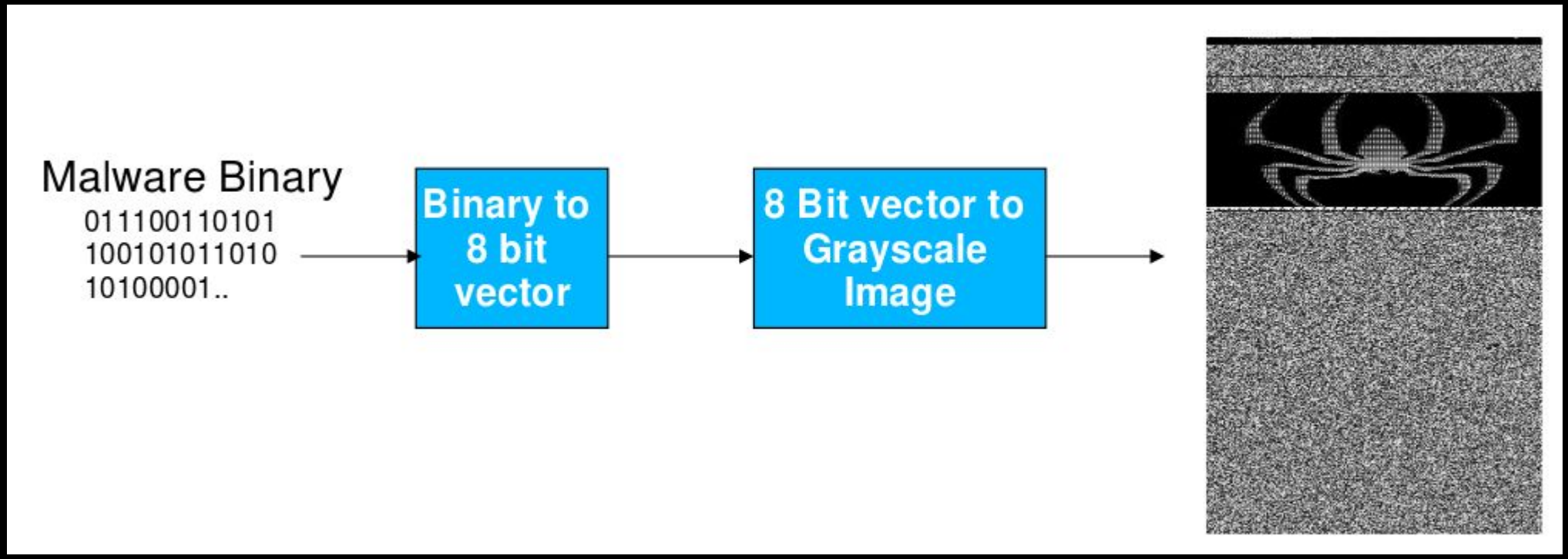
Malware Detection With Convolutional Neural Networks

- CNN의 강력한 Feature Extraction 성능에 기대



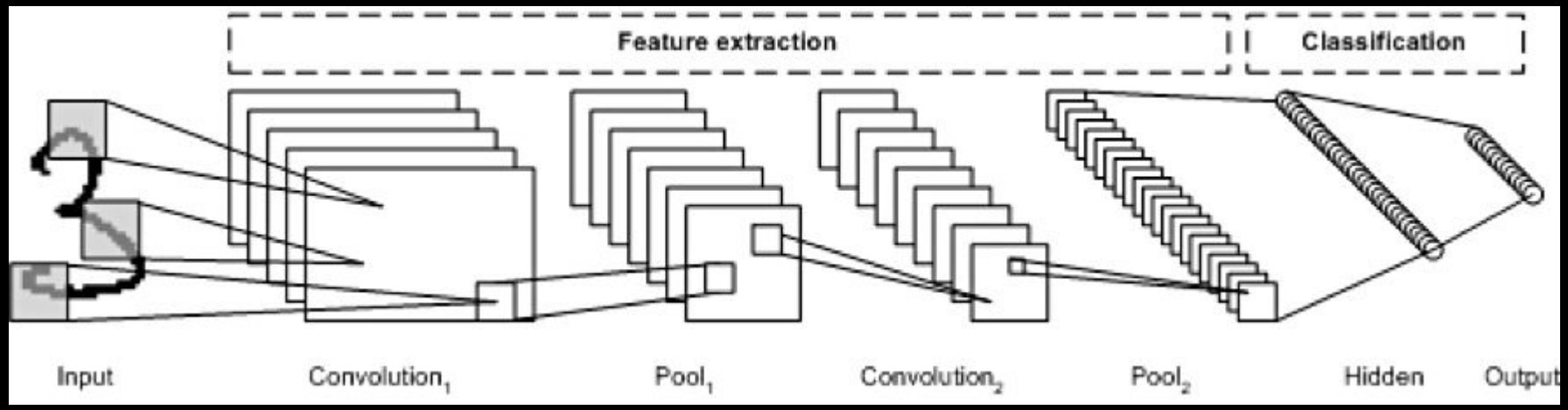
Malware Detection With Convolutional Neural Networks

- 바이너리 파일 → 그레이 스케일 이미지



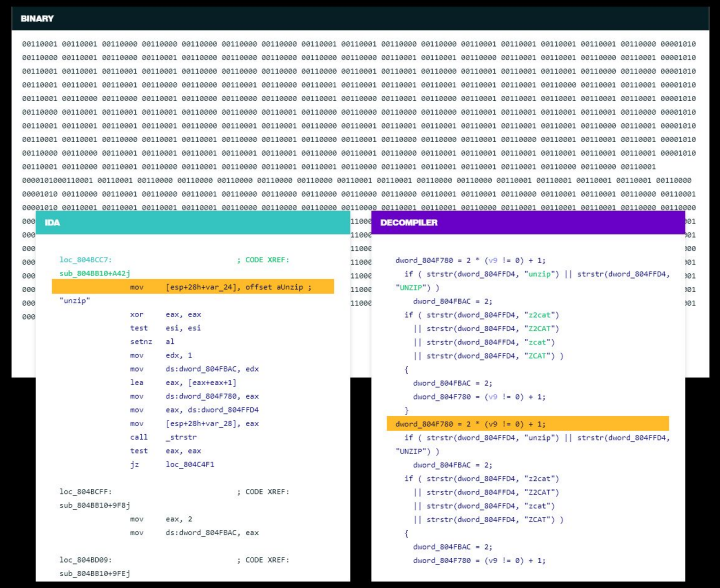
Compact feature hashing for machine learning based malware detection

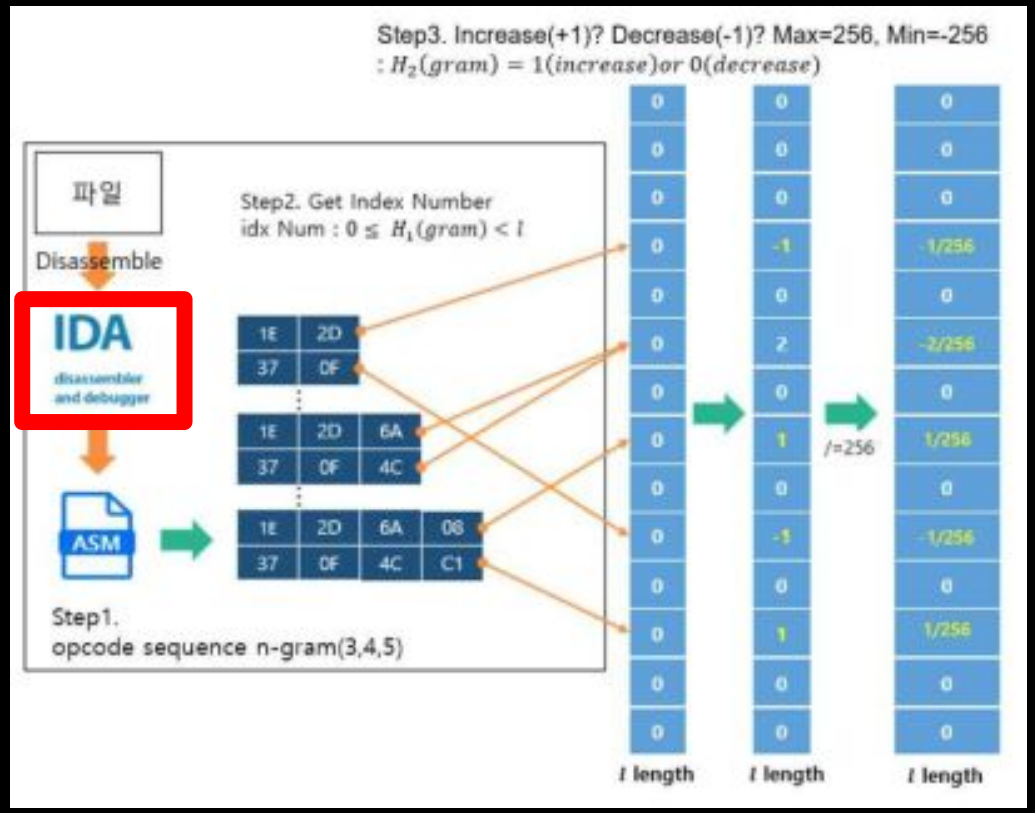
- CNN의 강력한 Feature Extraction 성능에 기대



Compact feature hashing for machine learning based malware detection

- 고정된 길이의 Input 값을 얻기 위해 Feature Hashing 사용





Q&A